Una mirada al criptoanálisis actual: tendencias y casos prácticos

Amparo Fúster Sabater

Dpto. Tratamiento de la Información y Codificación
Instituto de Física Aplicada, C.S.I.C.
C/ Serrano 144, 28006-Madrid
amparo@iec.csic.es

Se podría decir que existen tantos criptoanálisis distintos como criptosistemas puedan diseñarse. Sin embargo, las actuales técnicas criptoanalíticas pueden agruparse en diferentes familias que cubren el rango completo de criptosistemas encontrados en la literatura. Con el fin de presentar una panorámica amplia del Criptoanálisis actual vamos a señalar tres métodos criptoanalíticos bien diferenciados: la técnica de la "edit-distance generalizada" para el criptoanálisis de generadores binarios (cifrado en flujo), el denominado "slide attack" para el criptoanálisis de cifrados iterativos (cifrado en bloque) y el criptoanálisis de software criptográfico como el GNU Privacy Guard (Criptografía de clave pública).

1. La técnica de la "edit-distance" se aplica a cada uno de los posibles estados iniciales de los LFSRs que intervienen en el generador de secuencia. En la actualidad, se puede descartar un número amplio de tales estados "edit-distance generalizada" lo que permite mejorar sustancialmente la eficiencia y aplicabilidad de dicha técnica.

2. El "slide attack" es un procedimiento criptoanalítico para cifradores en bloque con un alto grado de autosimilaridad. Su fortaleza reside en que es independiente del número de vueltas (rounds) del cifrador. En la actualidad se ha aplicado con éxito al cifrador TREYFER, GOST así como a diversas variantes del BLOWFISH.

3. Este tipo de criptoanálisis no pone en tela de juicio la fortaleza de criptosistemas conocidos sino más bien cuestiona la fortaleza de *malas* implementaciones software de *buenos* criptosistemas, es el caso de la firma con ElGamal que aparece en el software GPG versión 1.2.3 incluída en muchas distribuciones de Linux.

Es ésta una visión general de los diferentes métodos criptoanalíticos que en estos momentos conforman el Criptoanálisis a nivel internacional.